

# Single photon generation by pulsed excitation of a single dipole

Rosa Brouri, Alexios Beveratos, Jean-Philippe Poizat, and Philippe Grangier

*Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS,*

*B.P. 147, F91403 Orsay Cedex - France*

*e-mail : jean-philippe.poizat@iota.u-psud.fr*

February 1, 2008

## Abstract

The fluorescence of a single dipole excited by an intense light pulse can lead to the generation of another light pulse containing a single photon. The influence of the duration and energy of the excitation pulse on the number of photons in the fluorescence pulse is studied. The case of a two-level dipole with strongly damped coherences is considered. The presence of a metastable state leading to shelving is also investigated.

PACS. 42.50.Dv, 03.67.Dd, 33.50.-j

## I. INTRODUCTION

The security of quantum cryptography is based on the fact that each bit of information is coded on a single quantum object, namely a single photon. The fundamental impossibility of duplicating the complete quantum state of a single particle prevents any potential eavesdropper from intercepting the message without the receiver noticing [1]. In this context, the realization of a efficient and integrable light source delivering a periodic train of pulses containing one and only one photon, would be an important advantage [2].

The purpose of this paper is to evaluate the reliability of such a source. Assuming that a smart eavesdropper can get the information as soon as the number  $n$  of photons in the pulse is larger than two (see Appendix 1), we define a fractional information leakage  $f_{il}$  as :

$$f_{il} = \frac{P_{n \geq 2}}{P_{n \geq 1}} \quad (1)$$

where  $P_{n \geq 1}$ ,  $P_{n \geq 2}$  are respectively the probabilities to get at least one and at least two photons. The value of  $f_{il}$  has to be close to zero, while the probability  $P_e = P_{n \geq 1}$  to emit one photon during the sampling period should be as high as possible; we note that the probability to get exactly one photon is  $(1 - f_{il})P_e$ . For a poissonian light source, we have:

$$f_{il} = 1 - (1 - P_e^{-1}) \ln(1 - P_e) \simeq \frac{P_e}{2} \quad (2)$$

$P_e \ll 1$

It is therefore possible to have a good reliability with an attenuated poissonian light source, but  $P_e$  has to be very small, which makes the source quite inefficient. A better way to have both a good reliability and high emission probability is to design a device with fully controlled quantum properties, able to emit truly single photon [3–11]. One possibility to perform such an emission is to use the fluorescence of a single dipole (e.g. a single molecule or a single colored center). As a single dipole cannot emit more than one photon at a time leading to antibunching in the photon statistics of the fluorescence light [12–14] a pulsed excitation of the dipole can be expected to produce individual photons on demand [3].

In previous works [4,5] the emitting dipole was generally considered to be a radiatively damped two-level system. In the present paper we will rather consider emitting dipoles with strongly damped coherences, as it is the case for single molecules [10] or single colored center [11] at room temperature. The decay time of coherences, associated to non radiative processes which occur in the picosecond range, is thus much shorter than the population decay time, that is typically in the 10 ns range. On the other hand, systems such as molecules or coloured centers often have an extra metastable state, which is very long lived and thus can induce “shelving” in the emission process. In order to describe these features, we will model the emitting dipole using the three level scheme shown in Fig. 1.

Owing to the fast damping of coherences, only level populations  $\sigma_{aa}$  will be considered, and the system’s dynamics will be described by using rate equations between the three levels. The system can be excited from ground state  $|1\rangle$  to excited state  $|2\rangle$  with a pumping rate  $r$ . The decay rate from level  $|2\rangle$  to level  $|1\rangle$  is  $\Gamma$ , but the system can also decay to a metastable state  $|3\rangle$  at rate  $\beta\Gamma$ . The branching ratio  $\beta/(1 + \beta)$  is usually (but not necessarily) very small. The emission rate from the metastable state will be neglected (*i.e.* no photons are emitted from level  $|3\rangle$ ), but we will assume that the system can go back from level  $|3\rangle$  to level  $|2\rangle$  with a rate  $r_d$ . This “deshelving” effect has been observed experimentally [15], and may be important under strong pumping conditions.

The purpose of the present calculation is to evaluate the efficiency of such a system in converting a train of classical light pulses into a train of single photon pulses (“photon gun”) [9]. We will thus assume that this system is excited by a train of light pulses of duration  $\delta T$ , such that  $\Gamma\delta T \ll 1$ . The separation between the pulses is denoted by  $T$ , with  $\Gamma T \gg 1$ . For ideal efficiency of the source, the dipole should be coupled to a field mode in a microcavity, which is then damped to the outside world. Here we will only consider free-space emission of the dipole, assuming that the emitted light is collected by purely passive ways, such as a parabolic retroreflector [7]. The corresponding imperfect detection efficiency will be included in the present model, but the possible effect of a microcavity will not be considered here.

In the following section, we will introduce a useful framework for carrying out the cal-

culatation. Then we will evaluate the quantities of interest, taking into account the detection efficiency. Finally we will present numerical results illustrating the behaviour of the system.

## II. THEORETICAL MODEL

### A. General framework

The evolution of the populations will be described using the diagonal terms of the density matrix  $\sigma_{bb}(t, t_0; a)$ , which denotes the population of level  $b$  at time  $t$ , starting from level  $a$  at time  $t_0$  (where  $a$  and  $b$  may take any value from 1 to 3). For the following it will be convenient to define the probability  $\sigma_{bb}^{(n)}(t, t_0; a)$  to go from state  $|a\rangle$  at time  $t_0$  to state  $|b\rangle$  at time  $t$ , with the emission of exactly  $n$  photons. The quantities  $\sigma_{bb}^{(n)}$  are linked to the populations  $\sigma_{bb}$  by the relation :

$$\sigma_{bb}(t, t_0; a) = \sum_{n=0}^{\infty} \sigma_{bb}^{(n)}(t, t_0; a) \quad (3)$$

The probability density to emit one and only one photon at time  $t$  when the system is in the state  $|a\rangle$  at time  $t_0$  is given by the probability  $\sigma_{22}^{(0)}(t, t_0; a)$  to be in the excited state at time  $t$  without any photon emission :

$$p_1 = \Gamma \sigma_{22}^{(0)}(t, t_0; a) \quad (4)$$

The quantities  $\sigma_{bb}^{(n)}(t, t_0; a)$  introduced previously can be related through the following recurrence relationship:

$$\sigma_{bb}^{(n+1)}(t, t_0; a) = \int_{t_0}^t \Gamma \sigma_{22}^{(n)}(t', t_0; a) \sigma_{bb}^{(0)}(t, t'; 1) dt' \quad (5)$$

In other terms, in order to emit  $(n+1)$  photons, the system has to emit the photon  $(n+1)$  at time  $t'$ , and to emit no photon from  $t'$  to  $t$ . The rate equations for  $\sigma_{bb}^{(0)}$  can be written :

$$\frac{\partial \sigma_{bb}^{(0)}}{\partial t}(t, t_0; a) = \sum_c r_{cb}^{(0)} \sigma_{cc}^{(0)}(t, t_0; a) \quad (6)$$

where similar equations hold for  $\sigma_{bb}$ , with coefficients  $r_{cb}$ . Using equations 3, 5 and 6, it can be shown (see Appendix 2) that the rate coefficients  $r_{cb}^{(0)}$  are related to the coefficients  $r_{cb}$  by:

$$r_{cb}^{(0)} = r_{cb} - \Gamma \delta_{b1} \delta_{c2} \quad (7)$$

where  $\delta_{ai}$  is one if  $a = i$ , and zero otherwise. For the three-level system we are considering in figure 1, we thus obtain the following rate equations:

$$\dot{\sigma}_{22}^{(0)} = r\sigma_{11}^{(0)} - (1 + \beta)\Gamma\sigma_{22}^{(0)} + r_d\sigma_{33}^{(0)} \quad (8)$$

$$\dot{\sigma}_{33}^{(0)} = -\Gamma_T\sigma_{33}^{(0)} + \beta\Gamma\sigma_{22}^{(0)} - r_d\sigma_{33}^{(0)} \quad (9)$$

$$\dot{\sigma}_{11}^{(0)} = -r\sigma_{11}^{(0)} + \Gamma_T\sigma_{33}^{(0)} \quad (10)$$

The difference between eq. 8 and the original rate equations for populations is the missing term proportional to  $\sigma_{22}^{(0)}$  in the last equation. This means that the ground level is no more filled after the emission of one photon, and ensures the uniqueness of the emitted photon.

Equations 8-10 allow, with the knowledge of the initial state, to derive the different quantities of interest. We first consider in subsection IIB the ideal situation of perfect collection efficiency. Subsection IIC deals with non-unity collection efficiency, which substantially modifies results of subsection IIB. Finally we take into account the effect of the metastable state in subsection IID.

## B. Two-level approximation with unit quantum efficiency

We assume first that all the emitted photons are detected (unit quantum efficiency), and that the dipole is initially in its ground state  $|1\rangle$ . Assuming also that  $\beta \ll 1$ , we can neglect the probability for the system to go to the metastable state in the time interval between two excitation light pulses, and set  $\sigma_{33} \approx 0$ . Eq. 8-10 therefore reduce to the following system :

$$\dot{\sigma}_{22}^{(0)} = r\sigma_{11}^{(0)} - \Gamma\sigma_{22}^{(0)} \quad (11)$$

$$\dot{\sigma}_{11}^{(0)} = -r\sigma_{11}^{(0)} \quad (12)$$

whose solutions are, for  $t \leq \delta T$ :

$$\sigma_{11}^{(0)}(t, t_0; 1) = \exp[-r(t - t_0)] \quad (13)$$

$$\sigma_{22}^{(0)}(t, t_0; 1) = \frac{r}{r - \Gamma} (\exp[-\Gamma(t - t_0)] - \exp[-r(t - t_0)]) \quad (14)$$

and for  $t \geq \delta T$ :

$$\sigma_{11}^{(0)}(t, t_0; 1) = \sigma_{11}^{(0)}(\delta T, t_0; 1) \quad (15)$$

$$\sigma_{22}^{(0)}(t, t_0; 1) = \exp[-\Gamma(t - \delta T)] \sigma_{22}^{(0)}(\delta T, t_0; 1) \quad (16)$$

The probability  $P_e^{(g)}$  to emit at least one photon between two pulses (say in interval  $[0, T]$ ) is then:

$$P_e^{(g)} = \Gamma \int_0^T \sigma_{22}^{(0)}(t, 0; 1) dt = 1 - \exp(-r\delta T) - \frac{r}{r - \Gamma} \exp(-\Gamma T) [1 - \exp((\Gamma - r)\delta T)] \quad (17)$$

This probability is of course increasing with the period  $T$ , which has to be large compared to  $\Gamma^{-1}$  to assure the emission of the photon (for instance,  $\exp(-\Gamma T) = 5 \cdot 10^{-5}$  for a 10 MHz pulse train and  $\Gamma^{-1} \approx 10\text{ns}$ ). We can therefore set:

$$P_e^{(g)} \approx 1 - \exp(-r\delta T) \quad (18)$$

The probability  $P_n^{(g)}$  to emit exactly  $n$  photons is given by:

$$P_n^{(g)} = \sum_a \sigma_{aa}^{(n)}(T, 0; 1) = \int_0^T dt \left\{ 1 - \Gamma \int_t^T \sigma_{22}^{(0)}(t', t; 1) dt' \right\} \Gamma \sigma_{22}^{(n-1)}(t, 0; 1) \quad (19)$$

where the second equality corresponds to the probability to emit the photon  $n$  at time  $t$ , and no photons within  $[t, T]$ . In the limit  $\exp(-\Gamma T) \rightarrow 0$ , the probability  $P_1^{(g)}$  is given by the following expression, which is well-behaved when  $r = \Gamma$ :

$$P_1^{(g)} = \left(\frac{r}{r - \Gamma}\right)^2 [\exp(-\Gamma\delta T) - \exp(-r\delta T)] - \frac{\Gamma r \delta T}{r - \Gamma} \exp(-r\delta T) \quad (20)$$

### C. Non-perfect collection efficiency

In practice, the dipole cannot be separated from the collection system, and the statistics of interest is the statistics of the detected events, rather than the one of the emission events. Assuming again that the initial state is the ground state, and denoting as  $\eta$  is the collection efficiency ( $\bar{\eta} = 1 - \eta$ ), the probability to collect no photon between  $[0, T]$  is :

$$\Pi_0^{(g)} = \sum_{n=0}^{\infty} \bar{\eta}^n P_n^{(g)} \quad (21)$$

Let us introduce the probability  $\tilde{\sigma}_{aa}$  to reach state  $|a\rangle$  without the collection of any photon, which is given by :

$$\tilde{\sigma}_{aa} = \sum_{n=0}^{\infty} \bar{\eta}^n \sigma_{aa}^{(n)} \quad (22)$$

From the above definitions, we have  $\Pi_0^{(g)} = \sum_a \tilde{\sigma}_{aa}$ . Using a calculation very similar to the beginning of this section (see eq. 7 and Appendix 2), the linear differential system for  $\tilde{\sigma}_{aa}$  can be shown to be :

$$\dot{\tilde{\sigma}}_{22} = r\tilde{\sigma}_{11} - \Gamma\tilde{\sigma}_{22} + r_d\tilde{\sigma}_{33} \quad (23)$$

$$\dot{\tilde{\sigma}}_{33} = -\Gamma_T\tilde{\sigma}_{33} + \beta\Gamma\tilde{\sigma}_{22} - r_d\tilde{\sigma}_{33} \quad (24)$$

$$\dot{\tilde{\sigma}}_{11} = -r\tilde{\sigma}_{11} + \Gamma_T\tilde{\sigma}_{33} + \bar{\eta}\Gamma\tilde{\sigma}_{22} \quad (25)$$

The correction introduced here, compared to equations 8-10, consists in the addition of a term filling the ground state with a rate corresponding to the probability density  $\bar{\eta}\Gamma$  to emit one photon but not to collect it. This term ensures the collection of one and only one photon. If the initial state is the ground state, and within the approximations of subsection IIB ( $\beta \ll 1$ ,  $\tilde{\sigma}_{33} = 0$ ), this system can be rewritten:

$$\dot{\tilde{\sigma}}_{22} = r\tilde{\sigma}_{11} - \Gamma\tilde{\sigma}_{22} \quad (26)$$

$$\dot{\tilde{\sigma}}_{11} = -r\tilde{\sigma}_{11} + \bar{\eta}\Gamma\tilde{\sigma}_{22} \quad (27)$$

This system can easily be solved between  $[0, T]$ , and we find for  $\Pi_0^{(g)}$ , in the limit  $\exp(-\Gamma T) \rightarrow 0$ :

$$\Pi_0^{(g)} = \tilde{\sigma}_{11}(\bar{\eta}; T, 0; 1) = \bar{\eta}\tilde{\sigma}_{22}(\bar{\eta}; \delta T, 0; 1) + \tilde{\sigma}_{11}(\bar{\eta}; \delta T, 0; 1) \quad (28)$$

with

$$\tilde{\sigma}_{11}(\bar{\eta}; \delta T, 0; 1) = \frac{r - \Gamma'}{r' - \Gamma'} \exp(-r'\delta T) + \frac{r' - r}{r' - \Gamma'} \exp(-\Gamma'\delta T) \quad (29)$$

$$\tilde{\sigma}_{22}(\bar{\eta}; \delta T, 0; 1) = \frac{r}{r' - \Gamma'} [\exp(-\Gamma'\delta T) - \exp(-r'\delta T)] \quad (30)$$

and

$$\begin{aligned} r' &= \frac{1}{2}(\Gamma + r + \sqrt{(r - \Gamma)^2 + 4\bar{\eta}r\Gamma}) \\ \Gamma' &= \frac{1}{2}(\Gamma + r - \sqrt{(r - \Gamma)^2 + 4\bar{\eta}r\Gamma}) \end{aligned} \quad (31)$$

The probability  $\Pi_0^{(g)}$  allows us to determine the probability  $\Pi_e^{(g)} = 1 - \Pi_0^{(g)}$  to collect at least one photon. It permits also to obtain the probability to collect one and only one photon :

$$\Pi_1^{(g)} = \sum_{n=1}^{\infty} n\eta\bar{\eta}^{n-1}P_n^{(g)} = \eta\partial_{\bar{\eta}}\Pi_0^{(g)} \quad (32)$$

We find thus :

$$\begin{aligned} \Pi_1^{(g)} &= \frac{\eta r}{r' - \Gamma'} \left( 1 + \frac{\Gamma(2\eta r - r - \Gamma)}{(r' - \Gamma')^2} \right) (\exp(-\Gamma'\delta T) - \exp(-r'\delta T)) \\ &+ \frac{\eta r \Gamma \delta T}{r' - \Gamma'} \left( \frac{r' - \eta r}{r' - \Gamma'} \exp(-\Gamma'\delta T) + \frac{\Gamma' - \eta r}{r' - \Gamma'} \exp(-r'\delta T) \right) \end{aligned} \quad (33)$$

These results correspond of course to the results of subsection II B if  $\eta = 1$ . A simpler expression can be obtained by considering in first approximation that no more than two photons can be emitted during the light excitation pulse. We then have :

$$P_0^{(g)} + P_1^{(g)} + P_2^{(g)} = 1 - P_e^{(g)} + P_1^{(g)} + P_2^{(g)} \approx 1 \quad (34)$$

Equation 21 can then be written as

$$\Pi_0^{(g)} = 1 - P_e^{(g)} + \bar{\eta}P_1^{(g)} + \bar{\eta}^2(P_e^{(g)} - P_1^{(g)}) \quad (35)$$

and equation 32 as

$$\Pi_1^{(g)} = \eta(P_1^{(g)} + 2\bar{\eta}(P_e^{(g)} - P_1^{(g)})) \quad (36)$$



### D. Influence of the metastable state

In order to study the effect of the metastable state, the 3-level equations given above can be solved analytically in the general case, giving lengthy and not very illuminating expressions. In physical terms, a short intense pulse will excite the dipole just as previously, but now the dipole may end up in the metastable state. Thus the emission of the single photon will be delayed by an amount depending on the time spent in the metastable state.

For definitiveness, we shall consider here the situation where the transition rate  $\beta\Gamma$  to the metastable level  $|3\rangle$  is weak but not completely negligible; this applies in particular to single molecules (see next section). The probability to populate this level when a transition occurs from level  $|2\rangle$  is  $\frac{\beta}{\beta+1} \approx \beta$ , so the metastable level is reached every  $(\beta P_e^g)^{-1}$  light pulses in average. In a way similar to the approximations of subsection II B, we can neglect the probability to leave the metastable state and to reach it again in the same cycle  $[0, T]$ . We can therefore neglect the filling term  $\beta\Gamma\tilde{\sigma}_{22}$  in equations 23, and the probability to stay in the metastable state in one cycle is  $\exp[-(\Gamma_M + r_d)T]$ , or for  $q$  cycles :

$$P_c = \exp[-(\Gamma_M + r_d)qT] \quad (37)$$

When the system reaches the metastable level, it therefore remains shelved during a mean time  $(\Gamma_M + r_d)^{-1}$ , that will be assumed to be much larger than  $T$ . The probability to reach this level is approximately  $\beta P_e^{(g)}$  for each excitation pulse, so the average time it takes for the system to find itself in the metastable state is  $T(\beta P_e^{(g)})^{-1}$ . The number of emitted photons is thus decreased by a factor

$$M = \frac{T(\beta P_e^{(g)})^{(-1)}}{T(\beta P_e^{(g)})^{-1} + (\Gamma + r_d)^{-1}} = \frac{(\Gamma + r_d)T}{\beta P_e^{(g)} + (\Gamma + r_d)T} \quad (38)$$

Even if  $\beta$  is small, the factor  $M$  can thus induce a reduction of the photon flux. Obviously this decrease in the number of emitted photons has different statistical properties than the random deletion considered in the previous section [16]. One gets now alternatively periods where the source is “on”, and periods where it is “off”. In a practical system, one may

consider to use a “deshelving” laser [15] in order to increase  $r_d$ , and thus to maximize the duty cycle of the dipole.

### III. DISCUSSION

In this section the above model is used to demonstrate the potentiality of a single emitter to produce single photons when excited by a light pulse. This potentiality is evaluated by the fractional information leakage  $f_{il}$  defined in Eq. (1). In particular the influence of the duration and the energy of the pulse is investigated. The parameters considered in the following corresponds to commercially available laser systems for typical emitters such as terrylene in *p*-terphenyl [10] or Nitrogen-Vacancy colored centers in diamond [11] with saturation intensity of the order of 1 MW/cm<sup>2</sup>. Note also that in all the plots discussed below the collection efficiency is taken as  $\eta = 0.2$ , which is a realistic value for an optimized passive collection system at room temperature.

In Fig. 2 the ability of the single emitter source to deliver truly single photons is compared to an attenuated Poissonian source with the same number of empty pulses. The fractional information leakage  $f_{il}$  is plotted as a function of the probability  $P_e$  of emitting at least one photon. The quantity  $P_e$  is varied by changing the pulse power while the pulse duration is kept constant. When the pulse duration  $\delta T$  is ten times shorter than the emitter’s lifetime, it appears that the occurrence of pulses with two photons or more is reduced by one order of magnitude when a single emitter is used instead of an attenuated Poissonian source. Reducing further the pulse duration to 1% of the emitter’s lifetime improve the fractional information leakage by another factor of 10.

Fig. 3 shows the influence of the pulse duration  $\delta T$  on the fractional information leakage  $f_{il}$  for a given excitation peak power (*i.e.* for a given  $r$ ). This would correspond to an experiment where the pulses are sliced up in a continuous wave laser with fast optical modulators. Of course the shorter the pulse the better  $f_{il}$ , but when the pulse is too short the probability  $P_e$  decreases also since the peak power is constant. Note that  $P_e$  can exceed

the collection efficiency  $\eta$  for  $\delta T$  large compared to  $\Gamma^{-1}$ . In this case the fluorescence pulse emitted by the dipole contains much more than one photon, so that even after the  $\eta = 0.2$  attenuation the probability of having more than one photon remains larger than  $\eta$ .

In Fig. 4 the fractional information leakage  $f_{il}$  and the probability  $P_e$  of emitting at least one photon are plotted versus the pulse power for a given pulse duration. As expected short pulses ( $\delta T = 0.01/\Gamma$ ) require more power to reach a value of  $P_e$  around  $P_e = \eta = 0.2$ , since  $P_e$  depends only on the pulse energy  $r\delta T$ . But short pulses offer a better fractional information leakage  $f_{il}$ , owing to the fact that the shorter the pulse, the lower the probability of emitting a photon and being reexcited within the same pulse.

For usual molecules or colored centers, the excited state lifetime is of the order of  $\Gamma^{-1} = 10$  ns, and typical saturation intensity when focussed on a sub-micron spot are of the order of 1 mW. For these types of emitting dipoles laser pulses with  $\delta T = 0.1$  ns and peak power of 1 W (ie pulse energy of 0.1 nJ) will already lead to good results. It has to be recalled that the incoherent model used here is valid only when the pulse duration remains larger than the coherence decay, that is in the picosecond range. This hypothesis prevents the use of extremely short and intense pulses, but is fully compatible with the numbers just quoted.

#### IV. CONCLUSION

We have evaluated the efficiency of a single photon source based upon the pulsed excitation of an individual dipole, in a regime where coherences are strongly damped and thus rate equations are relevant. This calculation applies for instance to the excitation of a single molecule or a single colored center at room temperature [11].

With respect to a radiatively damped two-level system, where either an exact  $\pi$ -pulse or a fast adiabatic passage is required [5–7], the requirement on the pulse intensity is much less stringent. This type of system is thus promising for achieving an all solid state single photon source operating at room temperature.

This work is supported by the European IST/FET program “Quantum Information Pro-

cessing and Telecommunication”, project number 1999-10243 “S4P”, and by France Telecom - Centre National d’Etude des Télécommunications under the “CTI” project number 99 1B 784.

## APPENDIX A: LOSS OF INFORMATION OWING TO PULSES CONTAINING TWO PHOTONS OR MORE IN A QUANTUM CRYPTOGRAPHIC SCHEME

We emphasize that  $f_{il}$  defined by eq. 1 clearly gives a physically meaningful evaluation of the single-photon character of the pulse. We note in particular that when  $P_{n \geq 1} \ll 1$ , the condition  $f_{il} < P_1/2$  is equivalent to the “anticorrelation” criterion  $\alpha < 1$  that was introduced in ref. [17]. We give below a few examples that suggest to conjecture heuristically that  $f_{il}$  also gives a good indication of the information leakage due to the multiphotonic character of the light pulses. The quantitative evaluation of  $f_{il}$ , which is the main result of this paper, obviously does not depend on the arguments given below.

For the sake of illustration, the information is supposed to be coded in the photon polarisation, but the following discussion remains valid for any types of information encoding. A simple strategy for Eve to exploit photon pairs is to tap a fraction  $\bar{\eta} = 1 - \eta$  of the beam, and to store the corresponding photons. The polarisation of the stored photons is measured later on, when Alice and Bob have disclosed the relevant basis information. Assuming that the probability to get more than two photons per pulse is negligible, the probability for Eve to catch the information is then  $2\eta\bar{\eta}P_2$ , which is maximum for  $\eta = 0.5$  and takes a value  $P_2/2$ . The relative fraction of Bob’s information which is known to Eve is then  $P_2/P_{n \geq 1}$ , which is just  $f_{il}$ . For attenuated light pulses, one gets  $f_{il} \approx P_2/P_1 \approx P_1/2$ . The action of Eve creates no polarisation errors, and cannot be distinguished from a 50% random loss in the transmission between Alice and Bob.

Another possible, more sophisticated strategy for Eve is to use a fast polarization-insensitive quantum non-demolition measurement [18] of the number of photons in each pulse, and to deflect every second photon. The polarization of the deflected photons is mea-

sured later on, as said above. The fraction of useful bits is thus  $P_{n \geq 1}$  for Bob,  $P_2$  for Eve, and the information leakage is again  $f_{il} = P_2/P_{n \geq 1}$ . This scheme introduces neither polarization errors, nor apparent loss. It can be nevertheless be detected by Bob if he analyses the photon statistics of the light pulses that he receives.

In presence of high transmission losses between Alice and Bob, for instance in long distance or free-space quantum cryptography, both methods can be combined to give even more powerful attacks [19,20]. For instance, let us assume that Eve is able to catch the light pulses before they go through the transmission line, and to distribute them to Bob through her own lossless line. Using the QND set-up, Eve identifies the pulses with more than one photon, keep one of them, and redistribute to Bob the remaining photons in order to simulate the low efficiency  $\eta_L$  of the original line between Alice and Bob. In that case, as soon as  $\eta_L < f_{il}$ , Eve gets essentially all the information and remains undetected. Though some countermeasures are possible, it is now clear that attenuated light pulses and high transmission losses are a deadly combination for quantum cryptography [19,20].

As a numerical example, when using attenuated light pulses with a typical value  $P_1 = 0.2$ , a fraction  $f_{il} = 0.1$ , *i.e.* at least 10% of the information may leak to Eve. By comparison, the single photon source described in this paper will give  $P_1 = 0.1$  and  $f_{il} = 0.002$  for experimentally reachable operating conditions ( $\Gamma\delta T = 0.01$ ,  $r = 1000\Gamma$ , overall efficiency 20%, see text for definitions). In the cryptographic situations discussed above, the information leakage to Eve is thus reduced by a factor 50 when using the single photon source.

## APPENDIX B: DERIVATION OF THE EQUATION FOR $\tilde{\sigma}_{BB}$ .

We will derive here the rate equations for the quantity  $\tilde{\sigma}_{bb}(\bar{\eta}; t, t_0; a)$ , which has been defined as :

$$\tilde{\sigma}_{bb}(\bar{\eta}; t, t_0; a) = \sum_{n=0}^{\infty} \bar{\eta}^n \sigma_{bb}^{(n)}(t, t_0; a) \quad (\text{B1})$$

Using this definition, we have:

$$\frac{\partial}{\partial t} \tilde{\sigma}_{bb}(\bar{\eta}; t, t_0; a) = \frac{\partial}{\partial t} \sigma_{bb}^{(0)}(\bar{\eta}; t, t_0; a) + \sum_{n=1}^{\infty} \bar{\eta}^n \frac{\partial}{\partial t} \sigma_{bb}^{(n)}(\bar{\eta}; t, t_0; a) \quad (\text{B2})$$

We have, for every  $n > 0$ , and from equation 5:

$$\frac{\partial}{\partial t} \tilde{\sigma}_{bb}(\bar{\eta}; t, t_0; a) \frac{\partial}{\partial t} \sigma_{bb}^{(0)}(\bar{\eta}; t, t_0; a) + \sum_{n=1}^{\infty} \bar{\eta}^n [\Gamma \sigma_{22}^{(n-1)}(t, t_0; a) \sigma_{bb}^{(0)}(t, t; 1) \quad (\text{B3})$$

$$+ \int_{t_0}^t \Gamma \sigma_{22}^{(n-1)}(t', t_0; a) \frac{\partial}{\partial t} \sigma_{bb}^{(0)}(t, t'; 1) dt'] \quad (\text{B4})$$

As we obviously have  $\sigma_{bb}^{(0)}(t, t; 1) = \delta_{b1}$ , and using eq. 6, we can rewrite eq. B3:

$$\frac{\partial}{\partial t} \tilde{\sigma}_{bb}(\bar{\eta}; t, t_0; a) = \sum_c r_{cb}^{(0)} \sigma_{cc}^{(0)}(\bar{\eta}; t, t_0; a) + \sum_{n=1}^{\infty} \bar{\eta}^n [\delta_{b1} \Gamma \sigma_{22}^{(n-1)}(t, t_0; a) \quad (\text{B5})$$

$$+ \sum_c r_{cb}^{(0)} \int_{t_0}^t \Gamma \sigma_{22}^{(n-1)}(t', t_0; a) \sigma_{cc}^{(0)}(t, t'; 1) dt'] \quad (\text{B6})$$

Using again eqs. 5 and 22, eq. B5 becomes

$$\frac{\partial}{\partial t} \tilde{\sigma}_{bb}(\bar{\eta}; t, t_0; a) = \delta_{b1} \bar{\eta} \Gamma \tilde{\sigma}_{22}(t, t_0; a) + \sum_c r_{cb}^{(0)} \tilde{\sigma}_{cc}(\bar{\eta}; t, t_0; a) \quad (\text{B7})$$

which is equivalent to eq. 23. Equation 7 can then be easily obtained by setting  $\bar{\eta} = 1$ , since  $\tilde{\sigma}_{bb}(1; t, t_0; a) = \sigma_{bb}(t, t_0; a)$ .

## REFERENCES

- [1] For a review see W. Tittel, G. Ribordy, and N. Gisin, *Physics World*, p. 41 (march 1998)
- [2] N. Lütkenhaus, *Phys. Rev. A* **59**, 3301 (1999); G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, *quant-ph/9911054*
- [3] F. De Martini, G. Di Giuseppe, and M. Marrocco, *Phys. Rev. Lett.* **76**, 900 (1996).
- [4] F. De Martini, O. Jedrkiewicz and P. Mataloni, *J. Mod. Opt.* **44**, 2053 (1997)
- [5] C.K. Law and H.J. Kimble, *J. Mod. Opt.* **44**, 2067 (1997).
- [6] S. C. Kitson, P. Jonsson, J. G. Rarity, and P. R. Tapster, *Phys. Rev. A* **58**, 620 (1998).
- [7] C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, *Phys. Rev. Lett.* **83**, 2722 (1999).
- [8] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, *Nature* **397**, 500 (1999)
- [9] A. Kuhn, M. Hennrich, T. Bundo, G. Rempe, *Appl. Phys. B* **69**, 373 (1999).
- [10] L. Fleury, J.-M. Segura, G. Zumofen, B. Hecht, and U. P. Wild, *Phys. Rev. Lett.* **84**, 1148 (2000).
- [11] R. Brouri, A. Beveratos, J.-Ph. Poizat and Ph. Grangier, to appear in *Optics Letters* (2000).
- [12] H. J. Kimble, M. Dagenais, and L. Mandel, *Phys. Rev. Lett.* **39**, 691 (1977).
- [13] F. Diedrich and H. Walther, *Phys. Rev. Lett.* **58**, 203 (1987).
- [14] Th. Basché, W. E. Moerner, M. Orrit, and H. Talon, *Phys. Rev. Lett.* **69**, 1516 (1992).
- [15] A. Dräbenstedt, L. Fleury, C Tietz, F. Jelezko, S. Kilin, A. Nizovtev, and J. Wrachtrup, *Phys. Rev. B* **60**, 11503 (1999).
- [16] J. Bernard, L. Fleury, H. Talon, and M. Orrit, *J. Chem. Phys.* **98**, 850 (1993).
- [17] P. Grangier, G. Roger and A. Aspect, *Europhysics Lett.* **1**, 173 (1986).

- [18] Ph. Grangier, J.-A. Levenson and J.-Ph. Poizat, *Nature* **396**, 537 (1998).
- [19] B. Huttner, N. Imoto, N. Gisin, T. Mo, *Phys. Rev. A* **51** 1863 (1995).
- [20] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, *Phys. Rev. Lett.* **81**, 3283 (1998); Comment by T. Durt, *Phys. Rev. Lett.* **83**, 2476 (1999).



## FIGURES

FIG. 1. Level scheme. The fluorescence is collected between level  $|2\rangle$  and  $|1\rangle$ . Level  $|3\rangle$  is a metastable state.

FIG. 2. Fractional information leakage  $f_{il}$  versus the probability  $P_e$  of emitting at least one photon for  $\eta = 0.2$ . The dashed and dotted lines correspond to the fluorescence of a single emitter, as described in the text, for different excitation pulse durations  $\delta T = 0.01\Gamma^{-1}$  (dashed line) and  $\delta T = 0.01\Gamma^{-1}$  (dotted line). The thin solid line is the fractional information leakage  $f_{il}$  for a Poissonian source.

FIG. 3. Influence of the pulse duration with  $\eta = 0.2$ . The pumping rate is kept constant,  $r = 100\Gamma$ . The thick line is the fractional information leakage  $f_{il}$ . The thin line is the probability  $P_e$  of emitting at least one photon. Both quantities are plotted versus the normalized duration of the exciting light pulse  $\Gamma\delta T$ .

FIG. 4. Influence of the pulse power. All traces are plotted versus the normalized pumping rate  $r/\Gamma$  for a given pulse duration  $\delta T$  with  $\eta = 0.2$ . The solid lines correspond to the fractional information leakage  $f_{il}$ , and the dashed lines to the probability  $P_e$  of emitting at least one photon. These values are given for  $\delta T = 0.01\Gamma^{-1}$  (thick lines) and for  $\delta T = 0.1\Gamma^{-1}$  (thin lines).

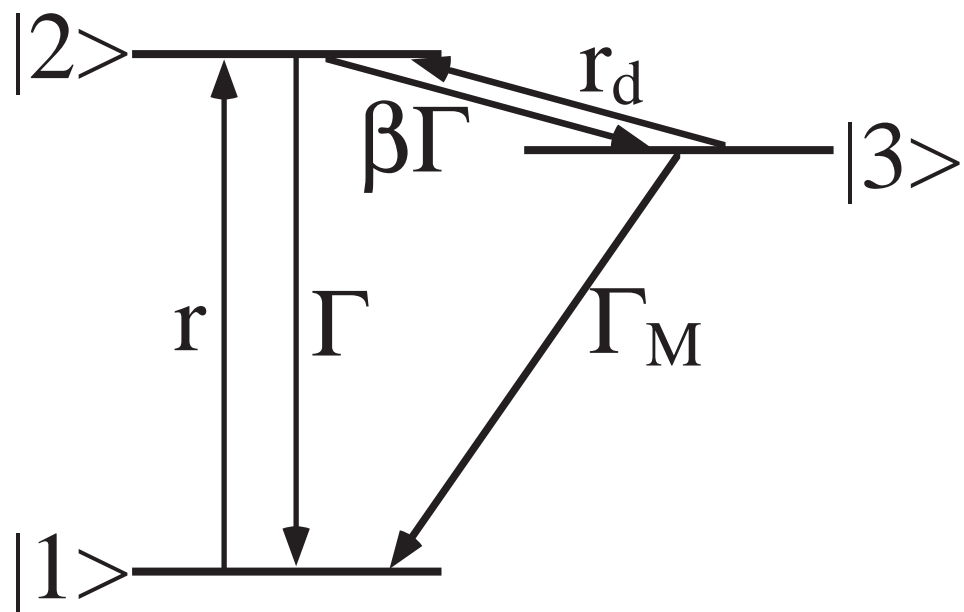


Fig.1 (Brouri et al)

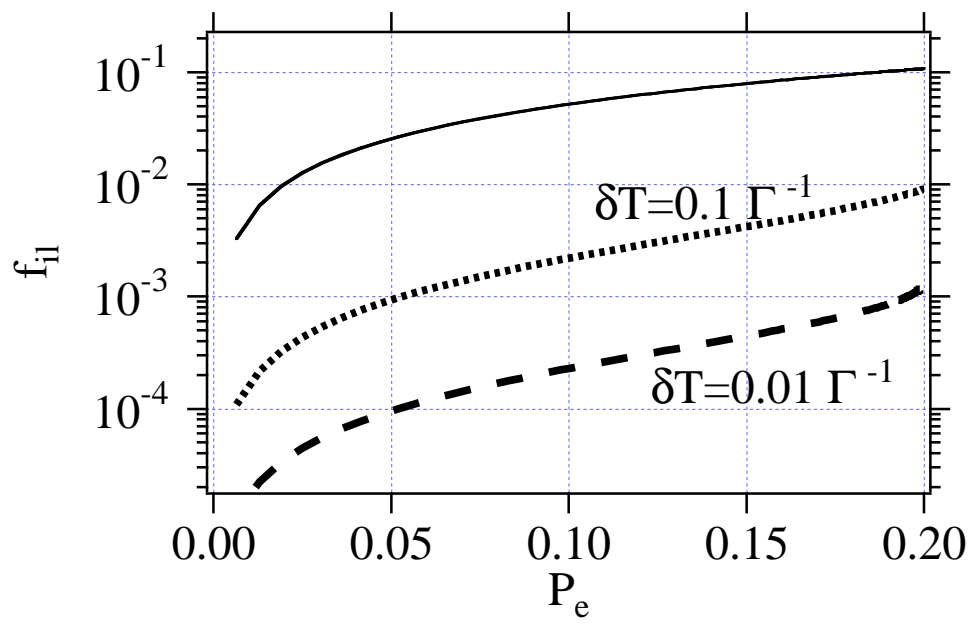


Fig.2 (Brouri et al)

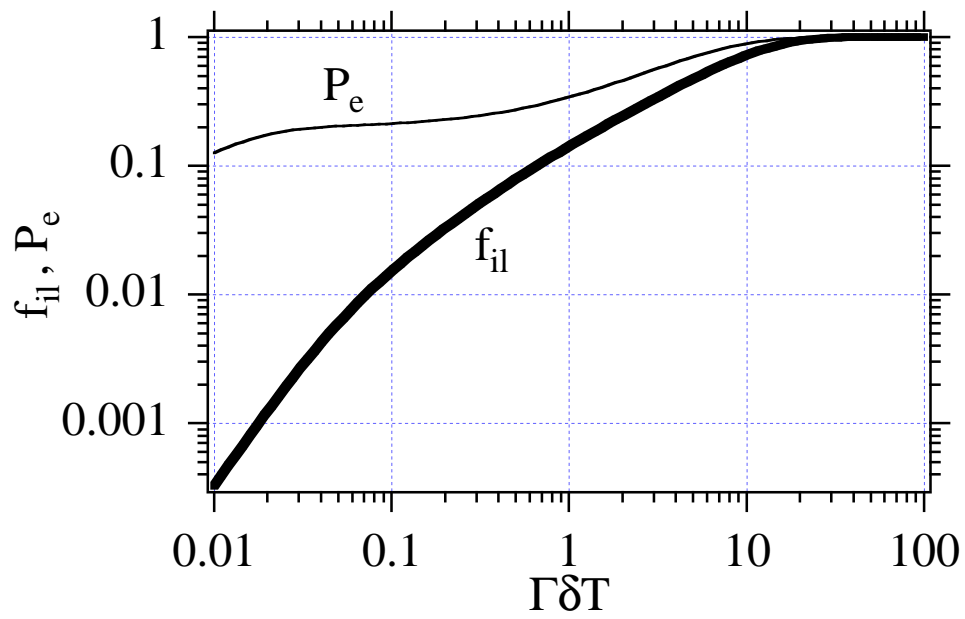


Fig.3 (Brouri et al)

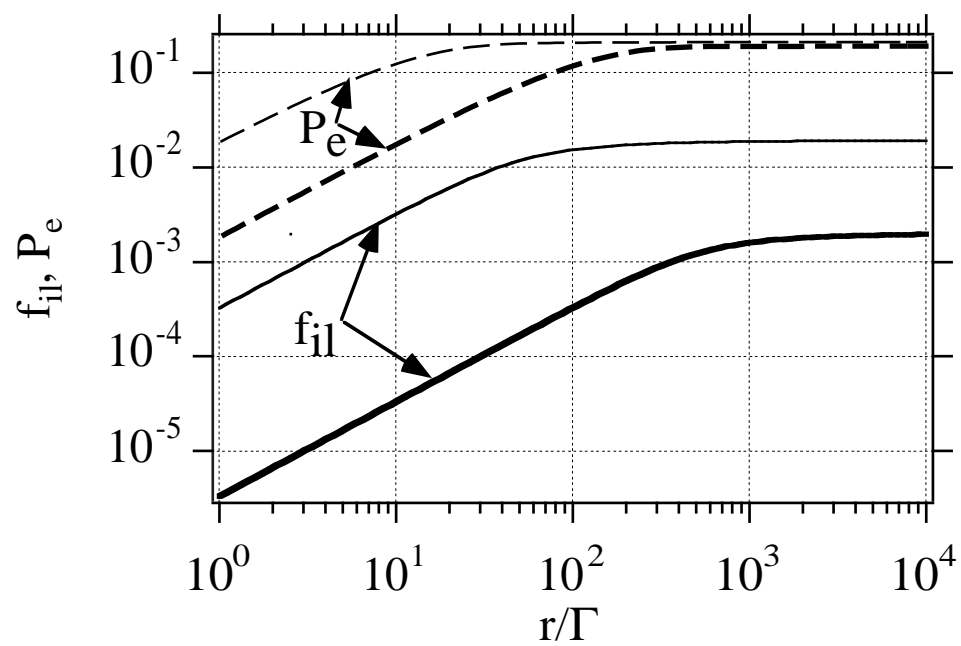


Fig 4 (Brouri et al)